Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D. C. 20554

CG Docket No. 04-53

In the Matter of

Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

REPLY COMMENTS OF CINGULAR WIRELESS LLC

J.R. Carbonell
Carol L. Tacker
M. Robert Sutherland

CINGULAR WIRELESS LLC
5565 Glenridge Connector
Suite 1700
Atlanta, GA 30342

Telephone: (404) 236-6364
Facsimile: (404) 236-5575

Counsel for Cingular Wireless

Date: May 17, 2004

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D. C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	CG Docket No. 04-53
Controlling the Assault of Non-Solicited	)	
Pornography and Marketing Act of 2003	)	

REPLY COMMENTS OF CINGULAR WIRELESS LLC

Cingular Wireless LLC (Cingular), through undersigned counsel, hereby submits its reply comments in the captioned proceeding. As discussed below, and for the reasons set forth in Cingular's Comments filed in this proceeding on April 30, 2004, Cingular supports the Congressional goal of eliminating unwanted mobile service commercial messages (MSCMs) and the Commission's efforts to implement Section 14 of the CAN-SPAM Act.[1]

I. The Responsibility for Compliance with the CAN-SPAM Act Rests on Senders of MSCMs.

The Commission must reject the effort of some commenters to shift the burden of compliance from the sender of MSCMs to wireless carriers and their customers. It was precisely to prevent senders of MSCMs from shifting the cost of eliminating wireless spam to wireless providers and their customers that Congress enacted Section 14.

In adopting the CAN-SPAM Act, Congress made it clear that the obligation of compliance is to be borne by the senders of MSCMs, not wireless providers or their customers. Specifically, Congress instructed the Commission to "determine how a *sender* of [MSCMs] may

[1] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub.L. No. 108-1187, 17 Stat. 2699 (2003) ("*CAN-SPAM Act*").

comply with the provisions of this Act…."[2] Despite this clear Congressional mandate some commenting parties representing marketers seek to shift the burden of compliance to wireless carriers and their customers. Thus, the National Association of Realtors (NAR) asks the Commission to impose an obligation to filter for MSCMs on wireless carriers.[3] The National Automobile Dealers Association (NADA) asks that the Commission require wireless carriers to provide customers with the means to "opt out" of future MSCMs.[4] While wireless carriers have every incentive to filter spam before it reaches their customers, Congress imposed on marketers the obligation to secure "express prior authorization" before sending MSCMs to wireless devices.

Intrado urges the Commission to adopt rules that encourage adoption of network-based filtering solutions that allow consumers and businesses to block or allow certain MSCMs.[5] Again, this would shift the burden of compliance from *senders* of MSCMs to *recipients* of MSCMs and their service providers. Nothing in the CAN-SPAM Act authorizes such a shift of responsibility. While the Commission can and should *encourage* wireless providers to adopt and continuously update anti-spam features, it cannot and should not make technology choices for carriers. These are private business decisions being made in a highly competitive marketplace.

One way to encourage wireless carriers to adopt aggressive anti-spam policies would be to find that the "safe harbor" provision of Section 230 of the Communications Act limits the liability of wireless providers against claims of blocking some lawful messages. No blocking software is perfect, and it is inevitable that some spam will get through and some legitimate messages will be blocked. CTIA notes that Congress has included in Section 230 protection for

[2] *CAN-SPAM Act* §14(b)(4).
[3] NAR Comments at 9.
[4] NADA Comments at 2. *But see* Motion Picture Association of America Comments at 4 (recognizing that Section 14 requires marketers to secure express prior authorization before sending a MSCM to a wireless device.")
[5] Intrado Inc. Comments at 3-4.

civil liability for those who block and screen offensive material.[6] The language of Section 230 is broad enough to cover a wireless service provider that filters spam aimed at customers of its short messaging service (SMS) and multimedia messaging service (MMS).[7] The Commission should affirmatively hold that wireless service providers that voluntarily filter spam on behalf of their customers are protected from civil suit under Section 230(c)(2).

Of the several proposals in the NPRM to facilitate identification of wireless subscribers, allowing wireless providers to provide a list of wireless domain names that marketers could access before sending MSCMs drew the most support among commenters. Nextel recommends that the Commission create a database of domain names that carriers use exclusively for mobile messaging. Marketers could consult the domain name and omit any addresses containing a mobile domain name unless it had received express prior authorization to contact the addressee. Nextel notes that this approach would facilitate enforcement against spammers.[8] Verizon Wireless also notes that senders of commercial e-mail should be able to discern whether the message is bound for a wireless handset from the domain name assigned to the service.[9] The various alternate proposals discussed in the NPRM were deemed too costly or impractical by

[6] CTIA Comments at 18, *citing* 47 U.S.C. § 230(c).

[7] The policy of Congress is clearly to encourage voluntary filtering and blocking of spam by end users and their service providers. Section 230(b)(3) states that it is the policy of the United States "to encourage the development of technologies which maximize user control over what information is received…" Section 230(c) is entitled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material." Section 230(c)(2) provides: "(2) CIVIL LIABILITY—No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be …otherwise objectionable, whether or not such material is constitutionally protected..." "Interactive computer service" is defined in Section 230(f)(2) as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server…" "Access software provider" in turn is defined in Section 230(f)(4) as "a provider of software (including client or server software) or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." SMS and MMS fit within the Commission's definition of "information services" and wireless service providers that utilize spam filters are properly considered "access software providers."

[8] Nextel Comments at 4-5.

[9] Verizon Wireless Comments at 18.

commenting parties. [10] Nextel spent the bulk of its comments demonstrating in detail how each of these alternative proposals is defective.[11] The Commission should heed these concerns and not impose technical requirements on wireless carriers.

The marketing associations also seek to shift the burden of compliance to wireless carriers on the basis that their members are small businesses. But the CAN-SPAM Act contains no exception for small businesses, and the Commission cannot exempt small .businesses from compliance with the Act. As commenting parties noted, spammers are predominantly small businesses, so creating a small business exception would eviscerate the protection that Congress intended for wireless subscribers.[12]

II. SMS and MMS Do Not Meet the Definition of MSCMs, and Are Not Covered by the Act.

Congress very carefully defined the type of messages that are subject to the CAN-SPAM Act. Section 14 of the Act applies to "mobile service commercial messages." In order to be a mobile service commercial message, a message must first be a commercial "electronic mail message."[13] The Act defines an "electronic mail message" as "a message sent to a unique electronic mail address."[14] "Electronic mail address" is defined as:

> a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an electronic mail message can be sent or delivered.[15]

Several commenting parties note that SMS and MMS messages do not meet the definition of

[10] Verizon Wireless Comments at 18; T-Mobile Comments at 19; CTIA Comments at 17;
[11] Nextel Comments at 5-15.
[12] T-Mobile Comments at 14-15; Nextel Comments at 15.
[13] CAN-SPAM Act § 14(d).
[14] CAN-SPAM Act § 3(6).
[15] CAN-SPAM Act § 3(5).

MSCMs because they are reached by dialing the wireless telephone number assigned to the device rather than an electronic mail address.[16] Parties arguing that the Act applies to these messages simply ignore the statutory definition of MSCMs.[17]

The fact that SMS and MMS messages are not covered by the CAN-SPAM Act does not mean that they are unprotected targets for spammers. As T-Mobile notes, these messages are protected by the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, because spammers cannot economically send spam to wireless devices without using an auto dialer. Customers can sue SMS spammers and the Commission can prosecute auto dialer users.[18] In addition, these types of messages are subject to "Do Not Call" registry protection.[19]

CTIA notes that wireless carriers have employed technical measures to prevent spam from reaching their SMS and MMS customers.[20] Verizon Wireless describes in detail the measures that it takes to protect its SMS and MMS customers from spam.[21] Dobson notes that attempts to send spam from one wireless device to another is impractical, because the use of wireless devices to send multiple messages is difficult and would be expensive, because the originating carrier would be billing the sender of the messages.[22]

III. The Commission Should Exempt Carrier-to-Customer MSCMs from the Requirements of Section 14(b)(1).

All of the carrier commenters agree that the Commission should exempt carrier to customer MSCMs from the requirements of Section 14(b)(1). There are good reasons for doing

[16] CTIA Comments at 7; T-Mobile Comments at 4; Dobson Comments at 4-5; Sprint Comments at 3.
[17] National Consumer League (NCL) Comments at 2; National Association of Attorneys General (Attorneys General) Comments at 4-5; Intrado Inc. Comments at 3. Electronic Privacy Information Center (EPIC) Comments 1-2.
[18] T-Mobile Comments at 5.
[19] Dobson Comments at 4-5.
[20] CTIA Comments at 8.
[21] Verizon Comments at 1-5.
[22] Dobson Comments at 5-6.

so and no good reason to the contrary. First, customers expect their wireless service provider to keep them informed about new products and services.[23] Any customer that does not want to receive such messages can simply 'opt-out" from all MSCMs or for a particular campaign. Dobson notes that MSCMs are one of the least intrusive means for a wireless carrier to contact its customers.[24] For some customers, such as prepaid customers, sending a message to the wireless device may be the only way to contact the customer.[25]

Second, Congress clearly contemplated that wireless carriers would be allowed to contact their customers without obtaining express prior authorization. Congress was aware that the Commission treated carrier-to-customer contacts differently than third party marketing in the context of the TCPA. While the TCPA expressly prohibited auto dialer and prerecorded messages to wireless phones, the Commission exempted wireless service providers from that prohibition, so long as the customer did not have to pay for the message.[26] Indeed, the very structure of 14(b) makes little sense if Congress intended that the exemption be denied. Why would Congress have conditioned the exemption on a carrier providing an opt-out option at the time service is established if at the same time the carrier was required to obtain express prior authorization from the customer?[27]

Congress told the Commission to take into consideration "the relationship that exists between providers of such services and their subscribers…"[28] In addition to the customer expectations noted above, the wireless service provider is in a unique position to suppress any

[23] CTIA Comments at 14.
[24] Dobson Comments at 12.
[25] Verizon Comments at 13; Nextel Comments at 18.
[26] Sprint Comments at 8-9; Nextel Comments at 17, *citing* Rules and Regulation Implementing the Telephone Consumer Protection Act of 1991, CC Docket No. 92-90, *Report and Order*, 7 FCC Rcd 8752, 8775 (1992).
[27] T-Mobile Comments at 17.
[28] CAN-SPAM Act § 14(b)(3).

charges for the messages it initiates to its customers.[29] No other marketer can do so. There is no danger that a wireless carrier will flood its customers with commercial messages. The wireless carrier can narrowly tailor contacts with the customer.[30] Any carrier that abuses it relationship with its customer through excessive marketing messages invites having the customer "opt out" of future messages, or to change carriers altogether.[31]

Commenters opposing the exemption offer no good reasons for doing so. EPIC complains that if the Commission grants wireless carriers the exemption "the burden will be on individuals to opt out."[32] This "burden" consists of nothing more than sending a reply message, contacting the carrier's customer service representative, or visiting the carrier's web site. NCL cites the statutory exception for 'transactional and relationship" messages as sufficient to meet the needs of wireless service providers. But as Dobson points out, the transactional and relationship exception is vague for mixed purpose messages, *e.g.*, a message that advises a customer about a new service option and provides the customer with a means to subscribe electronically.[33] The Attorneys General express concern that an exemption for CMRS providers "could make the statute susceptible to a constitutional challenge."[34] But as Verizon demonstrates, just the opposite is true. Verizon cites numerous cases in which courts have stricken down "opt-in" consent requirements where an "opt-out" requirement would be an adequate and less restrictive alternative in cases involving commercial speech.[35]

IV. Conclusion.

The Commission should place the burden of compliance with the CAN-SPAM right

[29] Dobson Comments at 12; Verizon Comments at 13.
[30] Dobson Comments at 13.
[31] CTIA Comments at 15.
[32] EPIC Comments at 8.
[33] Dobson Comments at 13.
[34] Attorneys Generals Comments at 8.
[35] Verizon Comments at 14-16.

where Congress intended it to be--on senders of MSCMs, not wireless carriers or their customers. The whole purpose of the CAN-SPAM Act is to prevent marketers from shifting the cost of their advertising from themselves to the target of the advertising. The Commission should recognize that SMS and MMS messages are outside of the scope of the CAN-SPAM Act. However, such messages are not a tempting target for spammers, and wireless carriers can protect their customers from any potential abuse over these services. Finally, the Commission should exempt wireless carriers from the requirements of Section 14(b)(1) of the CAN-SPAM Act, as Congress contemplated. There are excellent reasons for adopting the exemption and no good reasons to the contrary.

Respectfully submitted,

s/ M. Robert Sutherland
J.R. Carbonell
Carol Tacker
M. Robert Sutherland

CINGULAR WIRELESS LLC
5565 Glenridge Connector, Suite 1700
Atlanta, GA 30342
(404) 236-6364
Counsel for Cingular Wireless LLC

May 17, 2004

CERTIFICATE OF SERVICE

I, Lydia Byrd, an employee in the Legal Department of Cingular Wireless LLC, hereby certify that on this 17th day of May, 2004, courtesy copies of the foregoing Comments of Cingular Wireless were sent via first class mail, postage prepaid to the following:

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
9300 East Hampton Drive
Capitol Heights, MD 20743

John Muleta, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

In addition, the document was filed electronically in the Commission's Electronic Comment Filing System on the FCC website.

s/ Lydia Byrd
Lydia Byrd